Distributed Network Attack Detection System

Shreya Ray

GTU PG School,Gandhinagar

Abstract

Network attack detection is an important tool for information security. It is used to monitor networks for attacks or misbehaviour of the system and report these to the administration in order to take action. Basically, it detects some common attacks on network system. A signature based and anomaly based detection system will monitor the packets on the network and compare them against snort rules which is already predefined. If attacks are detected than it will generate the logs that are displays the list of attacks to the administrator for action. It also generates the alerts in the events of attacks directed towards on entire network. This is the research work and it is not fully implemented. The implementation of this research work is ongoing.

1. Introduction

With the development of network technologies and applications, network attacks are greatly increasing both number and severity. Internet has no boundaries. It is very important tool for information security. Security is a fundamental component of every network design.

There are two major categories in information Security. One is computer security that is protecting the files and information stored on the computer and another one is network security that is protecting the data during transmission in network. Network security is sometimes called Internet Security. Network attacks are comes into the network security.

1.1 Network Attacks [1]

Any computer connected to a network is potentially vulnerable to an attack. Attacks are mostly launched automatically without the owner's knowledge. Attackers have access to network communication between browser and server. Attacks may be launched to obtain or to steal the information.

Computer systems use a variety of components, ranging from electricity to power the machines to the software program executed via the operating system and that uses the network. There are various levels that present a security risk. Certain Risks are:

1.1.1 Physical access

This is a case where the attacker has access to the premises, and maybe even to the machines. Given Physical access to office, the knowledgeable attacker will quickly be able to find the information needed to gain access to the organization's computer systems and networks.

- Power outage
- Manual shutdown of the computer
- Vandalism
- Opening of the computer's case and theft of the hard drive
- Monitoring of network traffic

1.1.2 Communication interception

Attacker tries to intercept the communication and get some useful information when the packets are transmitted.

- Session hijacking
- Identity spoofing
- Re-routing or alteration of messages

1.1.3 Denials of service

In computing, a Denial of service attack is an attempt to make machines or network resource unavailable to its intended users. These are attacks aiming to disrupt the proper functioning of a service. Denials of service are usually broken down as follows:

- Exploitation of TCP/IP protocol weaknesses
- Exploitation of server software vulnerabilities

1.1.4 Intrusions

Intrusion attacks are those in which an attacker enters your network to read damage and steal your data. Intrusion detection system helps to identify the intrusions.

Snort is a lightweight and an open source network intrusion detection system. In that we have to make snort rules to detect the attacks.
Mainly two parts of rule:

- **Header**

Header portion of the rule mainly consists of the source and destination port, protocol and the actions to be taken.

- **Option**

Option Portion contains additional fields in the packets namely in the flags, content type, reference.

Examples of intrusion attacks are:

- Port scanning
- Elevation of privilege: this type of attack involves exploiting vulnerability in an application by sending a specific request, generating abnormal behavior that sometimes leads to system access with application rights. **Buffer overflow** attacks use this principle.
- Malicious attacks like viruses, worms and Trojan horses

1.1.5 Social engineering

Social engineering attack is one in which the intended victim is somehow tricked into doing the attacker's bidding. In this case, no protective devices can protect the user against spoofing. In addition to phishing, Social engineering attacks can come in many forms- email that masquerades or breaking news alerts or greeting cards, bogus lottery.

1.1.6 Trapdoors

It also referred as backdoors; it is a little bit of code that are embedded in programs by the programmers to quickly gain access at a later time.

1.1.7 Scanning and Exploits

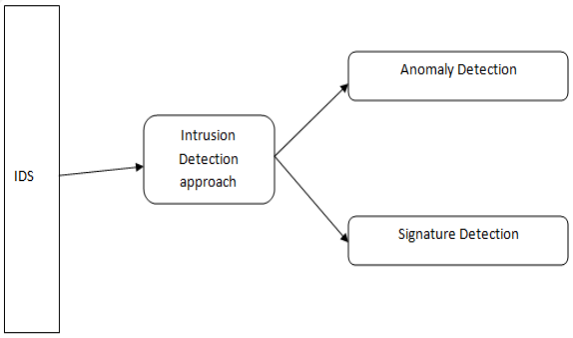
- scanning may include using search on Google
- more traditional methods like nmap

As a key technique in network security domain, Intrusion Detection System plays vital role of detecting various kinds of attacks and secures the networks. I will be more focused on intrusions Detection system. Snort as a network intrusion detection system open source code, can automatically monitor network data flow. It can be used for monitoring a variety of attacks and give detection and response to the distrustful events.

2. Intrusion Detection System

Due to the internet and local networks have become ubiquitous, the number of intrusion event has grown. Since some years, companies have put in several mechanisms to deal with the intrusions like firewall are used to filter the network traffic, antivirus is used to stop propagation of virus. But, these mechanisms have some limitations, thus the information systems have configuration breaches that allow the attacker to bypass the security mechanisms.

A firewall enforces which traffic is allowed in and out of the network, the firewall inspects the headers but not the contents of data packets. So, many exploits attempt to take advantage to find the weakness to launch the attack. That is why intrusion detection system is used for continuously monitoring the network traffic.



The most common approach to intrusion detection system is anomaly detection and misuse detection.

- **Anomaly detection**

It is described as statistically the user behaviour, in order to detect unusual behaviour or actions of the user like specific hours of logon and system activity.

- **Misuse detection or signature detection**

It is possible to create a generic signature that can detect the various attacks by matching it.

2.2 Related Work

Zhao Kai describes the idea is that unify the distributed detection and centralized management by the

hierarchical distributed structure. He divides the system in four parts. First part is Data Acquisition Subsystem that is also called as sensor and data analysis subsystem constitute data collection and analysis center. Second Part is Data Analysis Subsystem in which misuse detection and anomaly detection are used, which greatly improves inspection accuracy. Third Part is Console Subsystem that includes the process of collecting information and the exchange of information between consoles, method such as information encryption is used. Fourth part is Database Management Subsystem, is used for storing all the data. Whatever information is collected, all the event rules are stored in the database [3].

Kang Hong,Zhang Jiangang describes a distributed intrusion detection system based on self-similar traffic is designed and the specific implementation of all parts is presented. Self similar model consist five main components. **Network engine** that is based on Winpcap can capture original packets from network and from which to find the possible invasion or other sensitive information. **Host agent** collects information of various hosts, including log events. **Storage system** that is used to store the raw captured data. It is a shared database among different components of IDS. **Misuse detection engines** that analyses and processes raw captured data and the information provided by other parts. **Central console** that manages all the Data Acquisition and Analysis Center, displaying warning information of acquisition and analysis centers in a friendly, easy access way.[6]

3. Basic problems

These days mostly all the organizations are connected to the Internet, and are using the fundamental techniques for being safe against network attacks. Intrusion Detection devices are broadly used to detect such attacks. But these devices, having some human configuration flaw or some technical lacking, are not proving their best for providing security. If these devices are enhanced to provide better traffic filtering techniques and alert generation with advanced rules, they can be used as standalone devices against network attacks.

Threats Like direct attack on organization or individual and on a specific organization or widespread attack to detect any vulnerable devices. Due to increasing the network technologies, new malwares and attacks are found day by day. So intrusion detection system is not updated with latest patch. Sometimes anomalies that are hard to detect and signature can be passed.

It is done by professionals, newbies, revenge, hacktivists. It may done in many form like sending malwares, scanning network, exploiting vulnerabilities, parked domains, etc.

Exploiting vulnerabilities using some tools like CVE, nessus and the suspended domains may get parked on IPs belonging to the domain registrar, an organization from which the domain was originally bought. Parking IP address host several domains where either the newly bought domain is parked because the domain's owner has no built content yet, the domain was not renewed by the owner, in which case, the parked domain enters pending state, where the domain gets suspended owing to illegitimate activities. For domain registrar such as GoDaddy, 1&1etc. The set of parking IP is not always static which makes the identification of domains.

The prevalent systems are either having some patching flaw or maybe some signature missing for detecting the latest threat. If these flaws are repaired to have an up-to-date system, it can provide an updated security solution.

3.1 Monitoring the Network

Various methods and techniques are used for the intrusion detection purpose like Passive vulnerability scanner, Honey pot, Bro, Suricata, Snort etc. I will be going to use snort for detection.

Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods [13]. It divides into two parts: Header and option. Header portion contains the source and destination port, ip address where as the option portion contains additional fields like flag, msg, content etc. Snort is used primarily to passively monitor network traffic and generate alerts when threats are detected. All information will be stored on logs.

Why I am using snort?

- **Run continually:** The system must be reliable enough to allow it to run in the background of the system being observed.
- **Changing system behavior:** The system profile will change over time, and the Intrusion Detection System must be able to adapt.
- **Resist subversion:** The system can monitor itself to ensure that it has not been subverted.

3.2 Proposed Solution

The proposed work is to construct a distributed Intrusion detection system on each host. It consists to detect the network attacks from the publicly available network. The structure of the system where it is monitoring all the traffic which is coming on the basis of rules which are predefined. The system is capable to detect the attacks through the implementation of IDS. If the attack is detected then it will be stored on logs. Logs will be analyzed by the administrator. By developing python script we can automatically fetched port numbers, message, contents on the basis of details available and instantly create a rule and add it to the Snort engine with the updated details.

4. Conclusion

It captures packets transmitted over the network. The attack log displays the list of attack to the administrator for the action. By combining the rule based and signature based strategies of intrusion detection along with updated engine, a secure system for intrusion detection and monitoring can be established.

5. References

[1] Jim Binkley, Network attacks, Available:http://web.cecs.pdx.edu/~jrb/netsec/lectures/pdfs/attacks.pdf
[2]Parked domain, available: http://support.hostgator.com/articles/cpanel/what-is-a-parked-domain-how-do-i-create-and-delete-one
[3] Zhao Kai, "Research and Design of the Distributed Intrusion Detection System Based on Snort," iccsee, vol. 2, pp.525-527, 2012 International Conference on Computer Science and Electronics Engineering, 2012
[4] YingHui Peng," Research of Network Intrusion Detection System Based on Snort and NTOP", 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), IEEE, 2012, Page(s): 2764 - 2768
[5] Padmashani R, Shiju Sathyadevam, Devi Dath"Better Snort Intrusion Detection /Prevention System", 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012, Page(s): 46 – 51.
[6] Kang Hong,Zhang Jiangang,"An Improved Snort Intrusion Detection System Based on self-similar Traffic Model", Computer network and Multimedia Technology,2009.CNMT,2009. Page(s): 1 - 4
[7] Yung-Li Hu, Wei-Bing Su, Li-Ying Wu, Yennun Huang, Sy-Yen Kuo, "Design of event-based Intrusion Detection System on OpenFlow Network," dsn, pp.1-2, 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2013
[8] What it is Network intrusion detection, available: http://www.combofix.org/what-it-is-network-intrusion-detection-system.php
[9] Philippe Bunel,"An introduction to intrusion detection system", option 1 research on topics in information security, GIAC Essentials certification (GSEC), practical assignment, version 1.4c, SANS-conference-LONDON, June, 2004.
[10] Suricata-snort, Sebastien.damaye available: http://www.aldeid.com/wiki/Suricata-vs-snort
[11] Brian L. Tierney, Vern Paxson, James Rothfuss," An Overview of the Bro Intrusion Detection System", Lawrence Berkeley National Laboratory, available: http://crd-legacy.lbl.gov/DOEresources/SC04/Tierney_Bro_SC04.pdf

[12] Kurundkar G.D, Naik N., Dr.Khamitkar S.D," Network Intrusion Detection using SNORT", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.1288-1296
[13] Snort: www.snort.org